

Quantum secret sharing with two qubit bipartite mixed state

Satyabrata Adhikari *

*Department of Physics, Korea Advanced Institute of Science and Technology
Daejeon 305-701, Korea*

November 15, 2010

Abstract

Quantum secret sharing is one of the most important and interesting quantum information processing task. In quantum secret sharing, information is split among several parties such that only one of them is able to recover the qubit exactly provided all the other parties agree to cooperate. To achieve this task, all the parties need to share entangled state. As far as my knowledge, all the previous quantum secret sharing protocol used either pure tripartite or pure bipartite entangled state. In this work we use for the first time bipartite two qubit mixed state (formed due to noisy environment) in quantum secret sharing scheme. We further show that one party cannot extract the information without the collaboration of other party. We also study the property of the shared mixed state used in the quantum secret sharing scheme.

1 Introduction

Quantum entanglement [1] is one of the fascinating feature of quantum mechanics. There is no classical analog of quantum entanglement and that makes it more fascinating than anything else in physics. In the field of quantum information theory entanglement plays a major role. This is also a very useful resource in the sense that using entanglement one can do many things in the quantum world which are usually impossible in ordinary classical world. Some of these tasks are quantum computing [2], quantum teleportation [3], quantum cryptography [4] and quantum secret sharing [5]. In quantum secret sharing, quantum information encoded in a qubit is split among several parties such that only one of them is able to recover the qubit exactly provided all the other parties agree to cooperate. Therefore, quantum secret sharing is a very interesting quantum information processing task which was introduced in [5]. After its introduction, Karlsson et.al. [6] studied the similar quantum secret sharing protocol using bipartite pure

*tapisatya@gmail.com

entangled state. Many authors studied the concept of quantum secret sharing using tripartite pure entangled states [7, 8, 9, 10, 11]. Recently Q. Li et.al. [12] proposed semi-quantum secret sharing protocols using maximally entangled GHZ state which was shown to be secured against eavesdropping. Quantum secret sharing can also be realized in experiment [13, 14, 15, 16].

In this work we discuss the quantum secret sharing protocol in a following way: Let us suppose that a spy (Charlie) who is working under two commanders, Alice and Bob. Charlie's job is to sent the secret information to both the commanders. But Charlie suspect that one of the commanders is dishonest but he don't know who is the culprit (Alice or Bob)? i.e. he don't know who tries to find out the secret all by himself. So he decided to sent the secret information in such a way that one commander cannot collect the secret information without the help of other commander. How Charlie achieve this task is the main result of this work. To split information among two parties we use bipartite mixed state. Therefore, we discuss our quantum secret sharing protocol with two qubit mixed bipartite state. In section-2, we review generalised concurrence and quantify the maximum amount of entanglement present in Schmidt rank r pure state in $k \times k$ -dimensional system. In section-3, we study the pure state living in $k \times k$ -dimensional Hilbert space through the noisy environment. For two qubit system, we find that the mixed state (because of noisy environment) shared between two distant partners remains entangled if the concurrence of the initial entangled state greater than certain threshold value. In section-4, we use the two qubit mixed state (discussed in section-3) in demonstrating the quantum secret sharing protocol. In section-5, we end with conclusion.

2 Generalised Concurrence - A review

Hill and Wootters [17] introduced the first measure of entanglement for a pair of qubits and the name given to the entanglement measure is concurrence. For 2×2 - dimensional system, the concurrence for pure state is defined as

$$C(|\Psi_{AB}^{(2)}\rangle) = |\langle \Psi_{AB}^{(2)} | \sigma_y \otimes \sigma_y | (\Psi_{AB}^{(2)})^* \rangle| \quad (1)$$

Since $|\Psi_{AB}^{(2)}\rangle$ is a pure 2×2 bipartite state so it can be expressed in a Schmidt-decomposition form as

$$|\Psi_{AB}^{(2)}\rangle = \sqrt{\lambda_1}|00\rangle + \sqrt{\lambda_2}|11\rangle \quad (2)$$

where λ_1, λ_2 are schmidt coefficients and $\lambda_1 + \lambda_2 = 1$.

The concurrence (1) for the state (2) reduces to

$$C(|\Psi_{AB}^{(2)}\rangle) = \sqrt{2(1 - \text{Tr}(\rho_A^2))} = 2\sqrt{\lambda_1\lambda_2} \quad (3)$$

where $\rho_A = \text{Tr}_B |\Psi_{AB}^{(2)}\rangle \langle \Psi_{AB}^{(2)}|$ denotes the reduced density operator.

Rungta et.al. [18] then generalised the concurrence of two-qubit pure state to higher dimensional $k \times k$ system and the generalised concurrence (or *I-concurrence*) is defined as

$$C_I(|\Psi_{AB}^{(k)}\rangle) = \sqrt{\frac{k}{k-1}(1 - \text{Tr}(\rho_A^2))} \quad (4)$$

where $\rho_A = \text{Tr}_B |\Psi_{AB}^{(k)}\rangle\langle\Psi_{AB}^{(k)}|$, $|\Psi_{AB}^{(k)}\rangle = \sum_{i=1}^k \sqrt{\lambda_i} |i_A\rangle |i_B\rangle$, and $\sum_{i=1}^k \lambda_i = 1$. *I-Concurrence* can also be expressed in terms of Schmidt coefficients as [19]

$$C_I(|\Psi_{AB}^{(k)}\rangle) = \sqrt{\frac{S_2(\lambda_1, \lambda_2, \dots, \lambda_k)}{S_2(\frac{1}{k}, \frac{1}{k}, \dots, \frac{1}{k})}} \quad (5)$$

where $S_2(\lambda_1, \lambda_2, \dots, \lambda_k)$ is the 2nd elementary symmetric function of $\lambda_1, \lambda_2, \dots, \lambda_k$, i.e. $S_2(\lambda_1, \lambda_2, \dots, \lambda_k) = \sum_{i < j} \lambda_i \lambda_j$. Therefore, *I-concurrence* can be re-written as

$$C_I(|\Psi_{AB}^{(k)}\rangle) = \sqrt{\frac{2k}{k-1} \sum_{i < j, i, j=1}^k \lambda_i \lambda_j} \quad (6)$$

For 2×2 dimensional system, we have $C_I(|\Psi_{AB}^{(2)}\rangle) = C(|\Psi_{AB}^{(2)}\rangle)$.

But in reality, due to decoherence or due to preparation error, we generally have a mixed state. Therefore, the entanglement of the mixed state $\rho_{AB}^{(k)} = \sum p_i |\Psi_i^{(k)}\rangle_{AB} \langle\Psi_i^{(k)}|$ can be measured by convex roof extension method

$$C_I(\rho_{AB}^{(k)}) = \min \sum_i p_i C_I(|\Psi_i^{(k)}\rangle_{AB}) \quad (7)$$

where the minimum is taken over all possible decomposition of $\rho_{AB}^{(k)}$.

It is to be noted that the maximum amount of entanglement in 2×2 -dimensional pure system is unity. They are called maximally entangled state. Now if we proceed towards two pure qutrit entangled systems, then we can find two SLOCC inequivalent classes of states. The two inequivalent classes are Schmidt rank two class (SR-2) and Schmidt rank three class (SR-3). The pure states that belong to the Schmidt rank two class can have amount of entanglement at most $C_I(|\Psi_2^{(3)}\rangle) = \frac{\sqrt{3}}{2}$ ($|\Psi_2^{(3)}\rangle$ denote the pure state of Schmidt rank 2 in 3×3 -dimensional system) while pure SR-3 states can achieve the maximum amount unity. Therefore, all maximally entangled states in two qutrit system are Schmidt rank three (SR-3) states. Therefore, a obvious conclusion is that the amount of entanglement in any Schmidt number 2 state in two qutrit system is at most $\frac{\sqrt{3}}{2}$. Now it is important to ask a more general question that if we have a $k \times k$ dimensional entangled mixed state which has schmidt number r described by a density

operator $\rho_r^{(k)}$ then what is the upper bound of the amount of entanglement contained in $\rho_r^{(k)}$? The answer may be given as

$$\begin{aligned} (i) \quad & C_I(\rho_r^{(k)}) \leq 1, \text{ if } r=k \\ (ii) \quad & C_I(\rho_r^{(k)}) \leq [C_I(|\Psi_r^{(k)}\rangle)]_{max}, \text{ if } r < k \end{aligned} \quad (8)$$

where $|\Psi_r^{(k)}\rangle$ denotes the entangled pure state of schmidt rank r in $k \times k$ -dimensional system.

Theorem: If $|\Psi_r^{(k)}\rangle$ denotes the entangled pure state of schmidt rank r in $k \times k$ dimensional system, then

$$[C_I(|\Psi_r^{(k)}\rangle)]_{max} = \sqrt{\frac{k(r-1)}{r(k-1)}} \quad (9)$$

Proof: Since $|\Psi_r^{(k)}\rangle$ is a entangled pure state of schmidt rank r , so $|\Psi_r^{(k)}\rangle$ can be expressed as

$$|\Psi_r^{(k)}\rangle = \sum_{i=1}^r \sqrt{\lambda_i} |i_A\rangle |i_B\rangle, \quad r = 2, 3, \dots, k \quad (10)$$

The amount of entanglement in $|\Psi_r^{(k)}\rangle$ is measured by I - concurrence. Therefore

$$C_I(|\Psi_r^{(k)}\rangle) = \sqrt{\frac{2k}{k-1} \sum_{i < j, i, j=1}^r \lambda_i \lambda_j} \quad (11)$$

$C_I(|\Psi_r^{(k)}\rangle)$ can be maximized using lagrange's multiplier method subject to the constraint $\sum_{i=1}^r \lambda_i = 1$. We find that $C_I(|\Psi_r^{(k)}\rangle)$ attains its maximum value when $\lambda_1 = \lambda_2 = \dots = \lambda_r = \frac{1}{r}$. Therefore, the maximum value is given by

$$[C_I(|\Psi_r^{(k)}\rangle)]_{max} = \sqrt{\frac{k(r-1)}{r(k-1)}} \quad (12)$$

Hence proved.

Observations:

- (i) If $r=k$, then $[C_I(|\Psi_r^{(k)}\rangle)]_{max} = 1$, as expected.
- (ii) For higher dimensional system, i.e. as $k \rightarrow \infty$, $[C_I(|\Psi_r^{(k)}\rangle)]_{max} \rightarrow \sqrt{\frac{r-1}{r}}$
- (iii) For $k \times k$ - dimensional system, we have the following ordering of maximum value of I - concurrence for different schmidt rank states

$$[C_I(|\Psi_2^{(k)}\rangle)]_{max} < [C_I(|\Psi_3^{(k)}\rangle)]_{max} < [C_I(|\Psi_4^{(k)}\rangle)]_{max} < \dots < [C_I(|\Psi_k^{(k)}\rangle)]_{max} = 1 \quad (13)$$

3 Pure state through noisy environment

In this section we study the initially prepared pure state in $k \times k$ -dimensional system passing through the noisy environment. The state can only be used in some quantum information processing task if it is shared between two distant partners who wishes to exchange information between them. We assume that Charlie is the supplier of entangled states to two users Alice and Bob. The users of the entangled states always demand from the supplier for the maximally entangled state. But the supplier cannot fulfill their demand. Although supplier can prepare maximally entangled pure state in his laboratory but the problem is that he have to send the particles to its users through a noisy environment. In general, the noisy environment converts pure states to mixed states and hence the entanglement decreases in course of distributing the particles. Due to this reason, the users Alice and Bob have to satisfy themselves with lesser entangled mixed state compared to pure maximally entangled state.

Suppose that Charlie prepare a bipartite pure state $|\psi\rangle^{in}$ in $k \otimes k$ -dimensional system. Any bipartite pure state can be written in the Schmidt polar form as

$$|\psi\rangle^{in} = \sum_{i=1}^k \sqrt{\lambda_i} |i\rangle_1 \otimes |i\rangle_2 \quad (14)$$

where $\lambda_i > 0$, $i = 1, 2, \dots, k$ are the schmidt coefficients and satisfies the condition $\sum_{i=1}^k \lambda_i = 1$.

After creating the entanglement between two particles, Charlie then sent the particle 1 to Alice and particle 2 to Bob through noisy environment. In this work, the noisy environment is described by the unitary operator [20]

$$|i\rangle_a |0\rangle_E |M\rangle_x \rightarrow c |i\rangle_a |i\rangle_E |X_i\rangle_x + d \sum_{j \neq i}^k (|i\rangle_a |j\rangle_E + |j\rangle_a |i\rangle_E) |X_j\rangle_x \quad (15)$$

where $|0\rangle_E$ denote the initial state of the environment and $|M\rangle_x$ and $|X_i\rangle_x (i = 1, 2, \dots, k)$ denotes the ancilla states. The ancilla state vectors $|X_i\rangle_x (i = 1, 2, \dots, k)$ form an orthonormal basis of the ancilla Hilbert space.

Unitarity of the transformation (15) gives the following relation between the parameters c and d

$$c^2 + 2(k-1)d^2 = 1 \quad (16)$$

When both the particles 1 and 2 is being sent through the same noisy environment (15), the state (14) transform as

$$|\psi\rangle^{in} \rightarrow |\psi\rangle^{out} = c^2 \sum_{i=1}^k \sqrt{\lambda_i} [|i, i\rangle_{13} \otimes |i, i\rangle_{24} |X_i\rangle \otimes |X_i\rangle] + cd \sum_{i \neq j}^k \sqrt{\lambda_i} |i, i\rangle_{13} \otimes$$

$$\begin{aligned}
& (|i, j\rangle_{24} + |j, i\rangle_{24})|X_i\rangle \otimes |X_j\rangle + cd \sum_{i \neq j}^k \sqrt{\lambda_i}(|i, j\rangle_{13} + |j, i\rangle_{13}) \otimes |i, i\rangle_{24}|X_j\rangle \otimes |X_i\rangle \\
& + d^2 \sum_{i=1}^k \sqrt{\lambda_i} \left[\sum_{i \neq j}^k (|i, j\rangle_{13} + |j, i\rangle_{13}) \otimes \sum_{i \neq l}^k (|i, l\rangle_{24} + |l, i\rangle_{24})|X_j\rangle \otimes |X_l\rangle \right] \quad (17)
\end{aligned}$$

where $| \rangle_3$ and $| \rangle_4$ denote the qubit of the environment.

After tracing out the ancilla qubits, four qubit state is described by the density operator ρ_{1324} . When the sent qubit 1 (2) interact with its own environment qubit 3 (4), the state described by the density operator ρ_{13} (ρ_{24}) can be designated as local outputs. The local output is given by

$$\rho_{13}^{local} = \rho_{24}^{local} = c^2 \sum_{i=1}^k \lambda_i |i, i\rangle \langle i, i| + d^2 \sum_{i \neq j}^k \lambda_i (|i, j\rangle + |j, i\rangle)(\langle i, j| + \langle j, i|) \quad (18)$$

Since the state described by the density operator ρ_{14} (ρ_{23}) is formed between the sent qubit 1 (2) and environment qubit 4 (3) located at different place so they can be treated as non-local. The non-local output is given by

$$\begin{aligned}
\rho_{14}^{non-local} = \rho_{23}^{non-local} = & P \sum_{i=1}^k \lambda_i |i, i\rangle \langle i, i| + Q \sum_{i \neq j}^k \sqrt{\lambda_i \lambda_j} |i, i\rangle \langle j, j| + \\
& R \sum_{i \neq j}^k \lambda_i (|i, j\rangle \langle i, j| + |j, i\rangle \langle j, i|) + S \sum_{l, j \neq i} \lambda_i |j, l\rangle \langle j, l| \quad (19)
\end{aligned}$$

where $P = (c^2 + (k-1)d^2)^2$, $Q = d^2(4c^2 + 4cd(k-2) + (k-2)d^2)$, $R = d^2(c^2 + (k-1)d^2)$, $S = d^4$.

Alice and Bob then shared a state which is described by the density operator ρ_{14} (ρ_{23}). Let us now investigate the situation for $k = 2$ i.e. for two qubit systems.

In the computational basis $\{|1\rangle \otimes |1\rangle, |1\rangle \otimes |2\rangle, |2\rangle \otimes |1\rangle, |2\rangle \otimes |2\rangle\}$, the local and non-local output is given by

$$\rho_{13}^{local} = \rho_{24}^{local} = \begin{pmatrix} c^2 \lambda_1 & 0 & 0 & 0 \\ 0 & d^2 & d^2 & 0 \\ 0 & d^2 & d^2 & 0 \\ 0 & 0 & 0 & c^2 \lambda_2 \end{pmatrix} \quad (20)$$

$$\rho_{14}^{non-local} = \rho_{23}^{non-local} = \begin{pmatrix} P\lambda_1 + S\lambda_2 & 0 & 0 & Q\sqrt{\lambda_1 \lambda_2} \\ 0 & R & 0 & 0 \\ 0 & 0 & R & 0 \\ Q\sqrt{\lambda_1 \lambda_2} & 0 & 0 & P\lambda_2 + S\lambda_1 \end{pmatrix} \quad (21)$$

where $P = (c^2 + d^2)^2$, $Q = 4c^2d^2$, $R = c^2d^2 + d^4$, $S = d^4$.

Alice and Bob shared a mixed state described by density operator $\rho_{14}^{non-local}$ ($\rho_{23}^{non-local}$). Since charlie sent the two particles through the noisy environment so the state shared by the users Alice and Bob may or may not be entangled. It depends on the noisy environment. We will find that the shared state is entangled if there exist a critical value of the concurrence which measures the initial entanglement present in the two qubit pure system. This critical value of the concurrence depends on the parameter of the noisy environment. If the concurrence of initially prepared state less than the critical value then the shared state is separable. We use witness operator to find this critical value of the concurrence.

The optimal witness operator for two qubit system $W_1^{(2)}$ is given by [21]

$$W_1^{(2)} = \frac{1}{2\sqrt{3}}(I - \vartheta) \quad (22)$$

where ϑ can be expressed in terms of the pauli matrices σ_x, σ_y and σ_z as

$$\vartheta = \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z \quad (23)$$

In matrix form W can be re-expressed as

$$W_1^{(2)} = \begin{pmatrix} 0 & 0 & 0 & \frac{-1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 \\ \frac{-1}{\sqrt{3}} & 0 & 0 & 0 \end{pmatrix} \quad (24)$$

Therefore,

$$Tr(W_1^{(2)} \rho_{14}) = Tr(W_1^{(2)} \rho_{23}) = (\frac{-2}{\sqrt{3}})(Q\sqrt{\lambda_1\lambda_2} - R) \quad (25)$$

The non-local output $\rho_{14}^{non-local} = \rho_{23}^{non-local}$ is entangled if

$$Q\sqrt{\lambda_1\lambda_2} - R > 0 \Rightarrow 2\sqrt{\lambda_1\lambda_2} = C_I(|\psi\rangle^{in}) > C_I^{cr}(|\psi\rangle^{in}) = \frac{1+c^2}{4c^2}, \quad \frac{1}{\sqrt{3}} < c \leq 1 \quad (26)$$

Therefore, the critical value of the concurrence depends on the parameter of the noisy environment. Also we note that the function of the parameter c is a decreasing function so the critical value of the concurrence decreases as c increases. Thus, the lower value of the concurrence of the initially prepared entangled state may keep the non-local output shared state entangled if the noisy parameter c tends towards unity.

It is clear that the local output state described by the density matrix $\rho_{13}^{local} = \rho_{24}^{local}$ is separable because $Tr(W_1^{(2)} \rho_{13}^{local}) = Tr(W_1^{(2)} \rho_{24}^{local}) = \frac{1}{3\sqrt{3}} > 0$.

We should note that the optimal witness operator $W_1^{(2)}$ that detect the entangled mixed state described by the density operator $\rho_{14} = \rho_{23}$ is not unique. There exist another optimal witness operator [22] which produce the same result (26) is of the form

$$W_2^{(2)} = \frac{1}{2}(I - \vartheta) \quad (27)$$

where ϑ is given by (23).

Observation: If Charlie initially prepare a maximally entangled state, i.e. when $\lambda_1 = \lambda_2 = \frac{1}{2}$, then for some specific value of noisy parameter $c = \sqrt{2/3}$, the shared state between Alice and Bob takes the form of maximally entangled mixed state. The form of maximally entangled mixed state is given by

$$\rho_{23}^{non-local} = \rho_{14}^{non-local} = \begin{pmatrix} \frac{13}{36} & 0 & 0 & \frac{4}{18} \\ 0 & \frac{5}{36} & 0 & 0 \\ 0 & 0 & \frac{5}{36} & 0 \\ \frac{4}{18} & 0 & 0 & \frac{13}{36} \end{pmatrix} = \frac{4}{9}|\Phi^+\rangle\langle\Phi^+| + \frac{5}{36}I_4 \quad (28)$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Thus if maximally entangled pure state sent through noisy environment defined in (15) then there exist a value of the noisy parameter which transform the maximally entangled pure state to a maximally entangled mixed state which belongs to the family of Werner state [23].

4 Application of two-qubit bipartite mixed state in a quantum secret sharing problem

In this section, we discuss a protocol for quantum secret sharing using two-qubit bipartite mixed state. Our protocol can be described in a few step given below:

Step-I: Maximally entangled pure state prepared by Charlie

A *secret agent* called Charlie want to distribute his collected confidential secret to two senior officers called Alice and Bob in such a way that one officer (Alice/Bob) alone cannot gather all the confidential information by herself/himself. To accomplish his task, Charlie prepare a two qubit maximally entangled pure state either in the form $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or in the form $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. He would like to make his decision on $|\phi^+\rangle$ or $|\phi^-\rangle$ by tossing a coin. If "head" appears then he prepare $|\phi^+\rangle$, otherwise $|\phi^-\rangle$. We can designate "head" as "0" and "tail" as "1". In this way he encode one bit of information into the prepared state. Then he send one qubit to Alice and another qubit to Bob through a noisy environment defined by the unitary transformation (15). Because of the preparation strategy and noisy environment, Alice

and Bob shared a mixed state that described either by the density operator

$$\rho_{AB}^+ = \frac{P+S}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) + \frac{Q}{2}(|00\rangle\langle 11| + |11\rangle\langle 00|) + R(|01\rangle\langle 01| + |10\rangle\langle 10|) \quad (29)$$

or by the density operator

$$\rho_{AB}^- = \frac{P+S}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) - \frac{Q}{2}(|00\rangle\langle 11| + |11\rangle\langle 00|) + R(|01\rangle\langle 01| + |10\rangle\langle 10|) \quad (30)$$

where $P = (c^2 + d^2)^2$, $Q = 4c^2d^2$, $R = d^2(c^2 + d^2)$, $S = d^4$ and $c^2 + 2d^2 = 1$.

Step-II: Single qubit measurement performed by Alice

Alice then perform measurement on her qubit in the Hadamard basis $B_H = \{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. It is assumed that Bob also know about the measurement basis that Alice used. The single qubit state received by Bob after measurement depends on the outcome of the measurement.

(i) If the shared state is ρ_{AB}^+ and the measurement outcome is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned} \rho_B^{+0} &= \frac{1}{p} \text{Tr}_1 \left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}} \right) \otimes I_2 \right] \rho_{AB}^+ \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}} \right) \otimes I_2 \\ &= \frac{1}{4p} [I_2 + Q(|0\rangle\langle 1| + |1\rangle\langle 0|)] \end{aligned} \quad (31)$$

(ii) If the shared state is ρ_{AB}^+ and the measurement outcome is $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned} \rho_B^{+1} &= \frac{1}{p} \text{Tr}_1 \left[\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|-\langle 1|}{\sqrt{2}} \right) \otimes I_2 \right] \rho_{AB}^+ \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|-\langle 1|}{\sqrt{2}} \right) \otimes I_2 \\ &= \frac{1}{4p} [I_2 - Q(|0\rangle\langle 1| + |1\rangle\langle 0|)] \end{aligned} \quad (32)$$

(iii) If the shared state is ρ_{AB}^- and the measurement outcome is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned} \rho_B^{-0} &= \frac{1}{p} \text{Tr}_1 \left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}} \right) \otimes I_2 \right] \rho_{AB}^- \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}} \right) \otimes I_2 \\ &= \frac{1}{4p} [I_2 - Q(|0\rangle\langle 1| + |1\rangle\langle 0|)] = \rho_B^{+1} \end{aligned} \quad (33)$$

(iv) If the shared state is ρ_{AB}^- and the measurement outcome is $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned} \rho_B^{-1} &= \frac{1}{p} \text{Tr}_1 \left[\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|-\langle 1|}{\sqrt{2}} \right) \otimes I_2 \right] \rho_{AB}^- \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0|-\langle 1|}{\sqrt{2}} \right) \otimes I_2 \\ &= \frac{1}{4p} [I_2 + Q(|0\rangle\langle 1| + |1\rangle\langle 0|)] = \rho_B^{+0} \end{aligned} \quad (34)$$

where I_2 denotes the identity operator in 2×2 -dimensional Hilbert space and $p = \frac{1}{2}$.

(33) and (34) explains the fact that it is neither possible for Alice nor for Bob alone to decode the encoded information of Charlie. They only decode the information of Charlie when they both agree to collaborate with each other. If they agree to collaborate, then our protocol proceeds further to step-III.

Step-III: Alice declare the measurement outcome

After they agree to collaborate, Alice sent her measurement outcome to Bob.

- (i) If the measurement outcome is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ then she sent Bob a classical bit "0" and
- (ii) If the measurement outcome is $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ then she sent classical bit "1" to Bob.

Step-IV: Positive operator valued measurement (POVM) performed by Bob

When Bob receives the classical bit from Alice, he came to know about Alice's measurement outcome. Corresponding to each measurement outcomes, one of the two possible single qubit state may appear at Bob's site. To discriminate between the two possible single qubit state, Bob have to perform POVM on his received qubit. The constructed POVM at Bob's site is given by

$$\begin{aligned}\Pi_B^{(0)} &= \frac{1}{2}(I_2 + \frac{1}{Q}\sigma_x) \\ \Pi_B^{(1)} &= \frac{1}{2}(I_2 - \frac{1}{Q}\sigma_x)\end{aligned}\tag{35}$$

If Bob receives the classical bit "0" then Alice's measurement outcome should be $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Corresponding to the Alice's measurement outcome $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, Bob received either $\rho_B^{+0} = \frac{1}{2}[I_2 + Q(|0\rangle\langle 1| + |1\rangle\langle 0|)]$ or $\rho_B^{-0} = \frac{1}{2}[I_2 - Q(|0\rangle\langle 1| + |1\rangle\langle 0|)]$. Bob then perform POVM to detect the correct received state. POVM operators $\Pi_B^{(0)}$ and $\Pi_B^{(1)}$ discriminate the single qubit states ρ_B^{+0} and ρ_B^{-0} with certainty.

Similarly, if Bob receives the classical bit "1" then he can discriminate the single qubit state using POVM operators given in (35).

In this way our quantum secret sharing scheme work using two qubit mixed state.

5 Conclusion

Before we presented our main result, we have studied generalised concurrence or I-concurrence. We provide a compact formula to quantify the maximum amount of entanglement present in pure state of Schmidt rank r in $k \times k$ -dimensional system. We also have studied the $k \times k$ -dimensional pure state passing through a noisy environment. We then restrict ourselves to 2×2 -dimensional pure state and found that the

mixed state (because of noisy environment) shared between two distant partners remains entangled if the concurrence of the initial entangled state greater than certain threshold value. Thereafter, for the first time we discussed the quantum secret sharing protocol using two qubit mixed state which appeared due to noisy environment. Our quantum secret sharing protocol is very simple and may be realized in experiment. The noisy environment used in this protocol is nothing but can be described as a quantum cloning transformation. This type of transformation may be used by eavesdropper to steal information. Instead of quantum cloning transformation, one may use amplitude damping channel or any other decoherence processes.

6 Acknowledgement

I would like to thank Prof. H. S. Sim for discussion.

References

- [1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [2] C. H. Bennett, D. Divincenzo, Nature **404**, 247 (2000).
- [3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993); D. Bouwmeester, J-W Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature **390**, 575 (1997).
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
- [5] M. Hillery, V. Buek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999); R. Cleve, D. Gottesman, and H-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
- [6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
- [7] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000);
- [8] S. Bagherinezhad, and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
- [9] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
- [10] G. Gordon, and G. Rigolin, Phys. Rev. A **73**, 062316 (2006).
- [11] S. B. Zheng, Phys. Rev. A **74**, 054303 (2006).
- [12] Q. Li, W. H. Chan, and D-Y Long, Phys. Rev. A **82**, 022303 (2010).
- [13] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

- [14] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
- [15] C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Fortschritte der Physik **54**, 831 (2006).
- [16] J. Bogdanski, N. Rafei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).
- [17] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997), W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
- [18] P. Rungta, V. Buzek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).
- [19] G. Gour, Phys. Rev. A **71**, 012318 (2005).
- [20] V. Buzek, and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
- [21] R. A. Bertlmann, K. Durstberger, B. C. Hiesmayr and P. Krammer, Phys. Rev. A **72**, 052331 (2005).
- [22] A. Sanpera, D. Bruss, and M. Lewenstein, Phys. Rev. A **63**, 050301(R) (2001).
- [23] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).